TSINGCHIH

清智国际前沿动态

TSINGCHIH INTERNATIONAL FRONTIER TRENDS

【2022】 12月 [总第二期]

内部资料 注意保密

前沿战争科技研究

FRONTIER RESEARCH ON EMERGING WEAPONIZED TECHNOLOGIES

以知识创新推动社会进步

TSINGCHIH 清智 CONSULTING

本期主题介绍

2022年2月24日，俄罗斯开启对乌克兰采取特别军事行动，这也被西方社会认为是第二次世界大战以来欧洲最大规模的军事冲突。据军事观察家发现，高超音速飞行技术、无人机、游荡弹药、电子干扰技术、网络武器等新技术、新科技产品都在该战争中被大量应用，并引起了国际社会对军事科技与未来战争形态的关注甚至担忧。2022年美国发布的《国防战略》（National Security Strategy）指出，人工智能、量子科学、生物科技、网络和太空技术正在影响着未来战争的形态。前沿科技将持续把战争推向意想不到的方向，而战争也会把技术的发展带入新的领域，带来新的可能性。

国际上新兴技术在军事战争中的应用和发展不仅对中国领土安全带来了巨大挑战，也将敦促中国考虑长远的战略，研究制定军事科技的发展和治理政策，确保国际影响力和国家安全之间的平衡。本期选取了2021-2022年发布于美国国际战略研究中心（Center for Strategic and International Studies,CSCI）等国际知名智库的六篇研究报告及评论，通过整理提炼报告概要、主要观点和建议，试图介绍新兴战争科技的最新动态。这些报告介绍了人工智能、生物制药、太空、通信网络领域的前沿技术在军事战争中的应用，并从多维度分析了前沿战争科技研究引发的危机，展示了欧美国家视角下的治理思路。

在无人机方面，俄乌战争的双方将无人机大量地应用于情报侦察、精确打击和火炮引导等多个方面。今年2月乌克兰使用土耳其制造的TB2无人机在乌克兰南部赫尔松（Kherson）市上空精准击中了藏在树底下的俄军SA17地对空导弹系统。美国战略与国际研究中心（CSCI）发布的《空中反恐？如何长远地分析无人机》报告，全面分析了美国反恐行动中对攻击性无人机的依赖，指出无人机造成了大量无辜民众的伤亡。作者敦促拜登政府制定相关政策，综合考虑使用无人机的潜在后果、非攻击性用途等方面，以指导无人机在在军事中的应用。

除利用无人机进行空袭外，人工智能技术还被应用到了军事科技的方方面面。新美国安全中心（Center for a New American Security, CANS）发布的《人工智能与军备控制》报告探讨了人工智能在军事战争中的管控问题。文章指出，人工智能是一种被多领域广泛使用的新兴科技，绝对禁止人工智能在军事中的应用是不现实的，需要考虑特定的使用场景并从多个层面进行限制和管控。在俄乌战争期间，俄罗斯利用社交机器人散布恐慌并发出炸弹威胁，进而影响战事相关的舆论。俄乌双方也都利用人工智能技术对各种图像、语音情报进行分析。乌克兰应用美国企业Primer开发的人工智能工具在今年3月窃听到了俄罗斯士兵在战场上的通信内容。

在网络战争方面，俄罗斯在战争中多次针对乌克兰政务、金融、电信基础设施发动网络攻击。美国太空探索科技公司（SpaceX）为乌克兰提供星链（Starlink），通过巨大的卫星网络为乌克兰军队提供网络服务，保障上万台军事终端设备的正常运行。美国布鲁金斯学会（Brookings Institution）发布的《军事创新和技术变革：准备应对下一代的网络威胁》报告指出，未来20年内通信网络科技将会为战争带来前所未有的变革，美国军方在利用机器人和新兴通讯工具的同时，也需要做好准备，以应对对手在网络入侵上的威胁。

在生物科技方面，美国战略与国际研究中心（CSCI）发布的《基因组：故意操纵的时代开始了》报告指出，基因组操纵技术有巨大的前景和战略意义，不仅可以发展成一个有潜力的经济产业，还可以在军事中得以应用。报告分析了中美在该领域中的发展优劣，提出四点战略建议来促进确保美国在生物科技层面的安全利益。今年6月，俄军辐射、化学和

本期主题介绍

生物防护部队司令基里洛夫表示，美国国防部已承认资助了46个乌克兰生物实验室以及与乌克兰科学技术中心存在联系，俄军怀疑美国的目的是研发生化武器，并应用到未来的战争中。

面对各种各样的场景，基于国家的角度，我们应该如何正确评估前沿科技对未来战争的影响呢？美国兰德公司（RAND Corporation）发布的《2035年以后的新兴技术： 基于场景的未来军事突发事件技术评估》报告提出了一个技术评估框架，帮助美国陆军评估量子科技等前沿技术目前的发展是否能够应对未来极端环境下发生的战争（例如在北极地区与中国的战争），以帮助美军取得关键的胜利。该报告的技术评估框架和分析思路有广泛的参考和借鉴意义。

在太空科技方面，俄乌战争的双方不仅应用太空设备进行通信，还依靠太空定位、导航和定时系统进行精确攻击。俄罗斯的巡航导弹使用自己的格洛纳斯（GLONASS）定位卫星来寻找目标。美国也为乌克兰提供了利用GPS精准定位的海马斯（Himars）火箭和“神剑”（Excalibur）炮弹等武器以提高其精准攻击能力。英国下议院图书馆（House of Commons Library, UK Parliament）发布的报告《太空军事化》指出当下太空军事化、武器化的程度越来越高，报告介绍了国际上太空军事科技的发展现状并分析了美国等大国在该领域的优势。

值得注意的是，上述国际智库的报告主要基于美国（西方）的立场和国家利益出发，存在对中国的偏见和国际形势的认知偏差。本刊通过编译具有全球话语权影响力的国际智库的报告，目的是帮助我们更好地了解前沿战争科技研究的发展，更深入地理解军事科技的治理难题和未来战争的趋势，从而为我国政策研究和战略分析提供有益参考。

Contents

目录

空中反恐？如何长远地分析无人机

Counterterrorism from the Sky? How to Think Over the Horizon about Drones

■发布者：Erol Yayboke、Christopher Reid ■发布时间：2021年8月 ■发布机构：美国国际战略研究中心
（CSIS, Center for Strategic and International Studies）

摘要 ABSTRACT

在没有美军地面驻扎的国家，美国正在逐渐转向 "超视距"反恐行动（"over-the-horizon" counter-terrorism, OTH-CT），依靠遥控飞机/无人机（remotely piloted aircraft，RPAs）进行反恐活动。无人机一直是美国在相关行动中首选的监视和攻击工具，但对于在未来的反恐行动中是否部署无人机的问题，美国乃至国际社会仍然存在极大的担忧。无人机造成无辜民众伤亡，这削弱了美国反恐行动的合法性，也为极端主义组织的招募提供了理由。如果没有美军在地面驻扎，情报不足和分析误差等问题可能会进一步削弱依赖无人机的超视距反恐行动的有效性。随着超视距反恐战略的持续发展，拜登政府应该建立一个政策框架，综合评估使用无人机的潜在后果、无人机的非攻击性用途以及可以和其他技术配合使用的场景，从而决定是否使用无人机。在决定使用无人机的场景下，政府必须制定措施以确保无人机使用的透明性和可问责性，进而推动情报收集和共享机制的建立，保证民众的安全。

2013年5月13日，在大西洋上一架X-47B无人驾驶作战飞机被拖入乔治布什号航空母舰的机库。
（来源：美国海军，https://foreignpolicy.com/2022/01/05/over-the-horizon-biden-afghanistan-counter-terrorism/）

正文ARTICLE

2021年8月31日标志着美国在阿富汗二十年军事驻扎的结束。这一天也标志着美国在一个众所周知的极端主义暴力团体避难所，部署军事和情报收集机构的终结。在阿富汗和其它美国没有持续驻扎的地区，拜登政府宣布将反恐行动的重点转向 "超视距 "反恐，在没有其它情报收集机制的条件下，将主要依靠高空卫星技术和飞行机等离岸设备进行反恐行动。

因为使用无人机 (drones) 或 "遥控飞机" (remotely piloted aircraft, RPAs) 来袭击潜在的恐怖主义威胁可能会对一般民众带来影响，美国国会以及各个人权和人道主义组织对无人机的使用施加越来越大的压力。要真正落实拜登总统提出的 "有针对性的、精准的反恐战略"，政府就必须调和无人机进攻所带来的风险和影响，并解决人们对民众伤亡的担忧，让无人机军用有意义和正当化。

超视距反恐是基于对先进科技的信赖，认为无人机变得越来越精确，能够有效地提供信号情报 (SIGINT)，甚至取代地面上的军事行动，进而阻止在阿富汗、也门、北非等地的恐怖主义活动。相关政策制定者普遍认为，无人机的使用对美军既没有直接风险，也没有妨碍美军推动的在相关国家长期实地驻军的政治风险。然而，这种看法最终掩盖了无人机复杂的一面，让美国无法正确分析无人机的相关决策和战略所带来的风险，忽视了严重依赖无人机所带来的长期影响。

商业无人机的武器化在世界各地的冲突中被普遍使用，为全球带来威胁。
（来源：SecurityInfoWatch网站，https://www.securityinfowatch.com/perimeter-security/robotics/anti-drone-technologies/article/21277392/weaponization-of-commercial-drones-is-a-global-threat）

无人机不仅用于侦察，也成为反恐行动的首选武器

从军事角度看，无人机是实现"空中霸权"的一个宝贵工具，特别是在巡查方面。在性能上，它们远远超过了人驾军机（crewed aircraft），在巡逻现场拥有全方位的情报能力，并配合使用动态的武力攻击。武装无人机经常成为美国反恐行动的首选，特别是在阿富汗、利比亚、巴基斯坦、索马里和也门，无人机也成功在阿富汗消灭了“基地”组织（AI-Qaeda）的领导人。

当地面缺乏军事部署时，无人机可以持续在空中徘徊，操作简单，无可比拟。它们还可以有效地作为地面部队的空中掩护，也可以为捉襟见肘的空军提供支持。在乌克兰抵御最近一次的俄罗斯入侵时，许多专家认为俄罗斯在空战中比较有利，但土耳其制造的TB2无人机（Bayraktar TB2）让乌克兰有效地制衡了俄罗斯。无人机足以对抗一支传统军队的入侵，这表明无人机对抗野战部队是非常有效的。

短期的影响：无辜民众伤亡

尽管无人机在进攻上可以取得胜利，但由此产生的无辜伤亡为无人机的使用蒙上了阴影。美国海军分析中心（Center for Naval Analyses，CNA）的Larry Lewis博士在2013年的一项研究发现，一年之中无人机对阿富汗平民造成的杀伤是人驾军机的十倍。

据美国军方称，2014年8月至2021年6月，在空袭伊斯兰国家的行动中，有1417名平民在空袭中丧生，自2018年以来，至少有188名平民在阿富汗被杀。然而，《纽约时报》的一项调查显示，民众的伤亡情况被大大低估了，有数百人的死亡未被记录。智库“新美国”（New America）记录了巴基斯坦、利比亚、也门和索马里的无人机袭击事件，结合美国军方在伊拉克的数据和《纽约时报》的调查，发现自美国“911事件”以来，仅在这六个国家就有至少3000名平民被无人机误杀。

巴基斯坦、利比亚、也门和索马里的无人机袭击的估计伤亡人数

国家	无人机袭击总次数	预估平民伤亡人数(下限)	预估平民伤亡人数(上限)	预估总共伤亡人数(下限)	预估总共伤亡人数(上限)
巴基斯坦(2004–2018)	414	245	303	2366	3702
利比亚(2012–2020)	4606	637	930	1867	2482
也门(2009–2021)	376	125	151	1390	1779
索马里(2003–2022)	267	33	120	1483	1965
	5663	1040	1504	7106	9928

来源： 数据平台America's Counterterrorism Wars: Tracking the United States' Drone Strikes and Other Operations in Pakistan, Yemen, Somalia, and Libya（https://www.newamerica.org/international-security/reports/americas-counterterrorism-wars，最后更新于2021年6月17日）。

长期的后果: 带来心理伤害、损害美国反恐行动正当性、激化极端主义

在某些情况下, 部署无人机进行反恐的武力进攻, 对平民心理造成的伤害可能比恐怖袭击更大。这可能会危害区域稳定, 并煽动对美国的反感。无人机带来的影响超越了肉体上的伤害, 延伸到心理、经济和社会层面。无人机的遥控特性和隐蔽性使其既能有效地击杀目标, 又能在击杀目标所身处的广大民众中散播恐怖氛围。从2014年起, 瑞士非政府组织Alkarama调查了生活在部署了美国无人驾驶飞机地区的居民。在接受调查的100名居民中, 72人表现出许多创伤后应激障碍 (PTSD) 的症状。那些直接受到无人机袭击影响的人 (例如, 有近亲被杀) 和生活在该地区的居民被恐惧、失眠和不安情绪所困扰。这种恐怖的氛围不是因为暴力极端主义分子, 而是因为美国。

在过去的20年里, 美国无数的智囊团、政策专家和专业军事机构积极制定全球反恐战略。在这一过程中, 他们制度化了一些核心价值观, 如明确目标、赢得人心、引导舆论等。如果没有这些价值观, 很难想象美国能成功说服各国和民众, 让大家相信由美国及其盟友领导的全球安全战略优于由中国和俄罗斯主导的战略。

无人机的进攻正在推动恐怖主义, 促进了当地暴力极端主义组织发展。恐怖分子和极端主义组织可以利用平民的死亡来推进其宣传和招募工作。例如, 2020年的一项研究发现, 在无人机袭击恐怖分子后的几个月内, 更有可能发生恐怖分子的袭击。更直截了当地说, 用无人机进攻恐怖分子, 可能让平民更多地受鼓动投身到激进的恐怖行动中。

使用武装无人机的潜在风险

· 无人机经常被用于更困难的袭击任务, 在这些地方没有载人飞机, 或不愿意将士兵暴露在危险中, 或不知道最佳的交战时机, 导致军方过度依赖空中力量。

· 在缺乏人工情报和其它情报的情况下, 决策者可能会过度依赖过时的、有缺陷的或糟糕的空中情报 (例如, 模糊的图像可能导致他们将人误认为物体) , 从而导致确认偏差和过度依赖 "特征空袭" (signature strike) 。

不精准的特征空袭 (signature strike)

使用无人机的战略弊端在所谓的 "特征空袭 " (signature strike) 中表现得最为突出。由于无人机在巡逻过程中收集的信息, 以及由地面的军队和设备收集的信息往往不完善, 无人机攻击往往依赖已知恐怖主义分子和暴力极端主义分子的行为模式信息进行分析预测, 进而确定需要攻击的区域, 即通过"特征"定位。这种分析定位的手段被称为特征空袭, 最常在索马里、也门和巴基斯坦等地应用, 美国在这些地方既没有正式的军队部署也没有公开参与战争, 但有反恐的需求。与定点清除目标不同, 特征空袭不需要总统批准, 决策者往往不知道他们所针对的所谓恐怖分子或暴力极端分子的身份甚至人数。随之而来的不确定性和预测偏见, 无疑使民众的生命面临更大的威胁。需要注意的是, 只有更先进的无人机技术才可以让特征空袭变得精准有效。因此, 这是一个如何制定合理利用新技术的政策和战略问题, 而不是技术本身的问题。

在2021年8月, 美国武装力量从阿富汗的撤离期间非常混乱, 在呼罗珊 (Khorasan Province) 的一次袭击中, 13名美国军人和多达170名平民在喀布尔国际机场 (Kabul International Airport) 惨遭杀害。美军根据旧时的情报和目标的行动轨迹进行分析, 怀疑一辆白色丰田卡罗拉的司机携带爆炸物后, 军方官员对它当天的每一次停车都有预判, 最终决定实施一次致命的无人机特征空袭。五角大楼后来承认, 这次袭击误杀了10名平民, 包括7名儿童和司机, 而这名司机原来是在一个总部设在美国的人道主义组织工作的一名阿富汗雇员。

授权进行无人机袭击的人需要考虑造成民众伤亡的可能性。每当这些风险被认为是可以接受时, 还需要表明决策者的决定是符合国防政策、美军的联合条约以及涵盖军事必要性和人道主义等概念的国际法条约的。

如何决定是否使用武装无人机

1.**制定一个评估在空中反恐任务中使用无人机的政策框架, 考虑长期影响, 提高决策水平。**军事领导人需要考虑无人机的长期影响, 从而决定是否使用无人机进行攻击。要做到这一点, 可能需要提高审批权限, 并成立一个协调不同机构的工作小组, 小组由高级官员组成, 进行战略层面的决策。美国平民冲突中心 (Center for Civilians in Conflict) 主张这个机构需要由国家情报局局长和国家安全局、中央情报局以及国务院、司法部和国防部的高级官员组成。工作组还应与业务机构合作, 对无人机行动的长期及连带影响进行评估。正如兰德公司的一项研究所建议的那样, 这种评估机制的一部分应通过法律政策来体现, 取得风险、回报和遵守国际法之间的战略平衡。拜登政府在2021年初的临时决定应当被制度化, 要求必须经过高层批准才能在冲突区之外进行与反恐有关的无人机攻击。

2..**构建攻击网络, 而不仅仅是部署特征空袭。**空中反恐战略应强调使用无人机主要用于信号情报的收集, 禁止仅仅通过识别嫌疑人的行为模式作为武力攻击的依据。因此, 拜登政府应停止使用特征空袭, 美国国会应探索立法, 使无人机永远不能作为直接进行武力攻击的工具。定位特定的个人可能仍然是一种战术上的需要, 特别是当可靠的情报显示威胁迫在眉睫的情况下。然而, 一个更有效的超视距反恐行动应该专注于摧毁目标网络。虽然清除一个领导人或恐怖主义组织网络的中心可以在短期内挫败一个团体的行动, 但领导人是可以替换的, 这让恐怖主义威胁仍然存在。伊斯兰国和基地组织等有经验的组织拥有不透明的组织结构和应急计划, 它们已经学会了如何减轻领导层变化所带来的影响。在某些环境中缺乏地面人工情报 (human intelligence, HUMINT) 的情况下, 相较于无人机, 人驾空中侦察 (aerial reconnaissance) 可以绘制出团体之间的联系和行动, 为遏制恐怖主义网络提供更广泛、更综合的战略。

3..**使用一套更完整的技术工具。**无人机收集的数据应与太空情报、间谍情报和各种侦察设备收集的数据进行比较, 并应用人工智能和机器学习对现有数据进行分析, 形成参照。

如何正确使用无人机

1.**增强透明度和问责制。**关于使用无人机的政策和程序应该透明和公开。公众如何看待无人机的使用对制定交战规则、获得国际社会的认可、结成联盟、获得美军的准入以及赢得民众对美军的信任都有连带影响。由于美国正考虑向国际伙伴出售无人机，美国如何解释无人机的军用符合国际规范将变得越来越重要，这将为其他国家提供参考。

2.**改善情报收集和共享机制。**美国应加强与海外军事伙伴的合作，通过整合多种信息来源-包括空中侦察、信号情报和人工情报，将大大提高情报的准确性。无人机目前的配置有助于有效收集和汇总空中侦察信号情报。当这些信息得到实地人工收集的信息证实时，无人机可以成为有效的空袭力量。此外，对国际社会提供情报支持可以帮助我们维护人权和法治。在阿富汗，这可能意味着与法国或印度协调反恐战略，因为他们也希望遏制来自阿富汗的威胁。美国从阿富汗撤军后，中国和俄罗斯看到了与中东国家深化外交的机遇，因此美国应该优先考虑重新投身于建立与巴基斯坦等国的伙伴关系，以共同打击恐怖主义和暴力极端主义。

3. **最重要的是，保护民众。**避免民众伤亡是正确的，也是具有战略意义的事情。

作者信息

Erol Yayboke 是美国国际战略研究中心（CSCI）弱点与流动性项目（Project on Fragility and Mobility）主任兼高级研究员。

人工智能与军备控制

Artificial Intelligence and Arms Control

■ 发布者：Paul Scharre
Megan Lambert
■ 发布时间：2022年10月
■ 发布机构：新美国安全中心
（Center for a New American Security，CANS）

摘要 ABSTRACT

军备控制的成败取决于可取性（desirability）（即武器的军事价值与所感知的可怕程度）和可行性（feasibility）（即影响其成功的社会政治因素）。人工智能是一种具有无数非军事用途的赋能技术，这一特点将其与许多其他军事技术（如地雷或导弹）区分开来。由于人工智能被广泛使用，绝对禁止人工智能的所有军事应用是不可行的。然而，禁止或规范特定的使用场景是有可能的。本文为决策者当下限制人工智能在军事上应用提出了建议。

2022年8月17日，在德克萨斯州胡德堡，一名美国士兵在评估合成训练环境的虚拟集体训练器时调整他的虚拟现实头盔。
（图片来源：美国陆军，https://www.armyrecognition.com/weapons_defence_industry_military_technology_uk/soldier_insights_drive_us_army_development_of_mixed-reality_training_system.html）

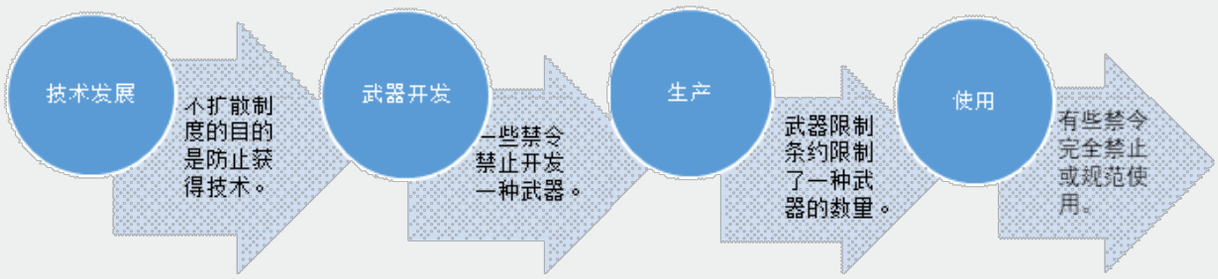
正文 ARTICLE

人工智能的进步给全球各政府的军队建设带来了巨大的机遇。伴随人工智能军事系统的发展，一些激进分子发出警告，呼吁限制或彻底禁止某些人工智能武器系统。相反，对人工智能军备控制持怀疑态度的人认为，作为一项在民用背景中被开发的通用技术，人工智能的发展将极难控制。

军备控制是什么

"军备控制"一般来说指的是各国为控制某些武器的研究、开发、生产、部署或使用而达成的协议。军备控制可以发生在武器开发和使用的各个阶段。如在技术发展阶段，核不扩散条约（nuclear nonproliferation treaty，NPT）等不扩散制度（nonproliferation regime）旨在防止发展某些武器背后的基本技术。在开发阶段，如地雷和集束弹药（cluster munition）等禁令允许军队获得相关技术，但禁止军队应用该技术开发、生产或储存武器。在生产阶段，军备限制条约（arms-limitation treaties）等条约允许生产某种武器，但限制各国在和平时期可以拥有的武器数量。在使用阶段，某些协议对战争中的武器使用进行规范，限制以某些方式使用武器或完全禁止使用武器。

贯穿武器开发和使用生命周期的军备控制措施



军备控制成功还是失败，取决于武器的可取性和可行性。军备控制的可取性指各国评估武器的军事价值和它的可怕程度（是否不人道、滥杀滥伤或破坏社会或政治秩序）。军备控制的可行性指影响军备控制成功与否的社会政治因素，包括国家明确所需限制程度的能力、国家遵守限制使用协议的能力、国家核查遵守情况的能力、以及确保协议成功所需要合作国家的数量。

人工智能是一种通用、新兴技术

人工智能是一种类似于电力或内燃机的通用赋能技术，而不是像潜水艇、膨胀子弹或致盲激光那样的独立的武器。从军备控制的角度来看，该技术的通用性带来了一些挑战。

首先，人工智能技术具有双重用途，既可用于民用，也可用于军事。该技术的扩散特性使得提议"封存"人工智能并减少其传播的不扩散制度不太可能成功。此外，由于人工智能技术的广泛存在，需要多个相关部门共同遵守军备控制制度，才能使军控有效。

其次，人工智能技术的通用性可能会使军备控制的要点不够明确。对于当今的人工智能技术而言，许多军事应用可能用于非武器用途，用以改进业务流程或操作效率，如预测设备是否需要维护、处理图像等，从而简化军事行动。可接受的军事人工智能用途和不可接受的用途之间的界限可能是模糊的，各国将需要明确所有相关协议才能让军控有效。

出于诸多原因，禁止所有军事应用人工智能不切实际，但限制人工智能的特定军事应用是可能的。那么问题是，哪些具体的军事人工智能应用是符合军备控制的可取性和可行性标准的？与核稳定（nuclear stability）、自动化武器和网络安全有关的人工智能应用已经成为学者们关注的焦点，可能还有其他重要的人工智能应用值得进一步考虑。禁令或条例可以针对被视为特别有问题的人工智能技术的具体实例进行严格管制，就像限制对在人体内爆炸的子弹，而不是所有爆炸的弹丸一样。

正如其他新兴技术一样，目前还不清楚人工智能将如何用于战争。军方认为人工智能是一种"改变游戏规则"的技术，这可能是实现军备限制的一个障碍。世界各地的军队都在投资人工智能，可能不愿意将一些应用限制在外。此外，对人工智能系统产生超人能力、精确性、可靠性和功效的认知可能会减少人们对某些人工智能应用可能破坏稳定或发生危险的担忧。即使一些人工智能应用最终被认为是需要被限制的，但如果它们已经被整合到军事部队或在战场上使用，实施起来可能会很困难。

核实AI合规性的挑战

与其他形式的软件一样，人工智能系统的核心属性不容易从外部观察到。为了让各国核实其他国家是否遵守军控协议，保持相互克制，可以考虑几种潜在的方法：

1.采用侵入式检查。各国可以允许第三方审查人员进入设施和特定军事系统，以验证其软件是否符合人工智能军备控制制度。然而，人工智能软件在被检查后可以迅速变更迭代，除非各国能够自信地克服人工智能快速更迭的特点，否则侵入性检查制度仍然不是验证合规性的有效方法。

2.**限制人工智能赋能系统的外部物理特性。**各国可以不关注系统的核心能力（传感器、硬件和软件等），而是关注易于观察和难以改变的总体物理特性，如尺寸、重量、功率、耐久性、有效载荷、弹头等。例如，如果各州担心攻击性无人机群的杀伤能力，相较于禁止人工智能技术在小型无人机中的使用，各州可以简单地禁止所有小型无人机作为军用武器。

3.**监管人工智能系统的可观察行为。**各国可以将监管集中在人工智能系统可观察的行为上。例如，各国可以制定规则，规范海军的自主水面舰艇（autonomous naval surface vessel）在接近其他舰艇时应该如何表现。

4. **限制计算基础设施的开发。**人工智能系统运用计算芯片作为物理基础设施。一方面可以限制人工智能硬件的开发，通过不扩散制度限制专用人工智能芯片来实现特定人工智能技术的发展。另一种方法将限制重点放在机器学习模型训练所需要的大规模计算资源（large-scale compute）上。

2020 年 9 月 1 日，美国内华达州内利斯空军基地，在高级战斗管理系统演习期间，Ghost Robotics Vision 60 原型机与一名安全部队飞行员一起在基地行走。该原型机使用人工智能和快速数据分析来检测并应对导弹或其他手段对国土的攻击。（来源：美国国防部，https://www.defense.gov/Multimedia/Photos/igphoto/2002547643/）

政策制定者当下可以通过限制人工智能硬件方面的发展，使全球人工智能技术在长期内更加可控。如果对全球供应链中的关键瓶颈实施出口管制可能有助于控制实现人工智能基础技术的传播，集中供应链并让未来的更加可控。然而，出口管制可能会加速技术本土化，因为那些被切断了重要技术的国家会加倍努力发展他们的技术能力。政策制定者在采用各种产业政策工具时应谨慎行事，以确保他们充分评估政策的长期后果。

作者信息

Paul Scharre是新美国安全中心（CNAS）副总裁兼研究总监。

军事创新和技术变革：准备应对下一代的网络威胁

Military Innovation and Technological Change: Preparing for the Next Generation of Cyber Threats

■ 发布者：Micheal E. O'Hanlon ■ 发布时间：2022年1月 ■ 发布机构：布鲁金斯学会（Brookings Institution）

摘要 ABSTRACT

本研究指出对数字技术及包括机器人和现代军事通信在内的相关系统正在快速发展。如果一场军事革命要在2022年和2040年之间发生，它将被数字领域推动。如果美国和其他民主国家要避免在科技竞争中败下阵来，美国必须重视网络领域的漏洞，保证不能让自己遭受致命的破坏性攻击。

美国军方网络安全专家正在确保像B-52轰炸机上的航空电子系统不会成为网络攻击者的目标。（来源：Military Aerospace，https://www.militaryaerospace.com/trusted-computing/article/14073852/military-cyber-security-tactical-network）

正文 ARTICLE

从现在到2040年，美国及其盟友，以及他们的对手，在网络领域的军事创新上，最大的机会点在哪里?最大的弱点会在哪里?回答这两个问题可以确保美国和其他民主国家不会对他们的对手感到担心。这份简报试图展望未来大约20年，推断出届时技术可能达到的水平。总体的预测是，与军事创新有关的技术变革在未来20年内可能比过去20年的发展更快、影响更广泛，而这种可能性主要由网络领域驱动。鉴于包括俄罗斯等多个国家现在拥有与西方国家在军事创新竞争的资源，美国和盟国应该重新解决网络领域的主要漏洞，以应对未来可能来自他们的攻击。

通讯

现代军队，特别是美国及其主要盟国的军队，极其依赖战场上大量的数据传送，以支撑正常的军事行动。这种依赖的形成主要是由于计算机、光缆和其他传播技术在对抗基地组织、伊斯兰国组织和塔利班的战争中显得非常有效。

未来的新兴技术可能会进一步辅助战术、战区和战略通信。例如，激光通信系统可以发挥重要作用，特别是在云层和其他障碍物不构成阻碍的空间内。无线电设备的能力会越来越强，它们附带的先进计算机可以最终协调从一个频率到另一个频率的跳频。移动通信的创新和允许"网络跳跃"等高效通信的先进网络，将使通信网络更加强大和可靠，足以抵御特定类型的破坏。

计算机

在计算机方面，技术可能会持续快速地发展。利用现存的计算能力，无数的应用将继续被发明出来，在许多领域有巨大的开发潜力。未来计算机领域的发展将加速转向多核处理器和专业芯片的研发。

例如，计算能力的提高可以让众多卫星和其他传感器通过各种算法和人工智能自动整合数据。这些类型的多平台网络可以帮助降低反卫星武器攻击大型高价值军事资产的风险。如果美国国防部（Department of Defense，DOD）通过像国防创新单位（Defense Innovation Unit，DIU）这样的单位成功建立与硅谷等计算机产业发达地区的联系，这类科技将更快取得突破。

FORCECON 2022是一个互动的工业和学术界碰撞的活动，参与者可以与工业和小企业顾问联系。（来源：美国空军，https://www.af.mil/News/Article-Display/Article/3046295/forcecon-2022-spurs-collaboration-innovation-for-air-force-industry-academia）

机器人技术

由于计算机领域带来的变革，机器人技术将继续大幅发展。自动驾驶已经成为可能，很快会有一些为特定军事目的（如在战场上提供战术补给）特别制造的车辆。美国陆军的"翼人"（Wingman）就是一个例子。翼人正在被改造用于承载武器，至少用于测试环节（尽管在决策环节有真正的人类士兵参与）。俄罗斯和土耳其等国家，也在推动这一技术领域的发展。

其他具有更具体功能的机器人也会被建造，这些机器人会拥有先进的传感器系统，通常以网络或无人机群（swarms）的方式行动。在空中，机器人技术可能用于制造隐蔽的无人驾驶飞行器（unmanned aerial vehicles，UAVs）。现在，可以飞行10小时和100公里的无人机只需几十万美元，而射程在一公里以内的四旋翼飞机（quadcopter）只需几百美元。在海上，未来的机器人技术的应用可能包括无人水面舰艇（unmanned surface vessel），用于情报收集、扫雷，以及局部点防御，以应对快速攻击潜艇。水下机器人设备（unmanned underwater vehicles，UUVs），如国防高级研究计划局（Defense Advanced Research Projects Agency，DARPA）的"海上猎人"（Sea Hunter），可以执行与反潜战和地雷战有关的搜索功能。一些无人潜航器即使在靠近敌人海岸的地方也可以保持持久运作和低信号。一架价值10万美元的海洋滑翔机最近穿越了大西洋，未来的研发可能会让水下机器人的成本降低10倍。

在某些情况下，机器人将可能被赋予使用武力的决策权，但需要道德审视和法律监督，相关的风险也很大。由于军事行动必须要快，这将激励人们在许多战术环境中让机器参与决策。例如，在陆地、空中或水中以群组形式运作的小型机器人可以被赋予一定的权限，以决定何时发挥其攻击能力。机器人通过相互沟通，实时处理有关敌人的信息，集中攻击防御最薄弱的地方。其他类型的无人机群可以攻击停放的飞机，就算是发动小型爆破，经过精确引爆，也可以使机翼或发动机失效，或产生二次爆炸。考虑俄罗斯和中国在这方面的进展，美国是否会成为主导者还不清楚。

具有人工智能的机器人也可以在战场上与人类形成紧密合作。这些机器人和人类可以一对一地配对，或以更大的数量，为一个士兵或一个团队服务。以色列在2020年使用远程遥控机器杀害了一名伊朗核武器科学家，这个事件引起了关注，预示了机器人与军队的合作。

网络的脆弱

随着计算机技术的进步，网络变得越来越脆弱。美国无疑拥有世界上最好的、最顶尖的网络进攻能力。这些能力可以用来对付军队的计算机和网络，以及其他国家更广泛的经济和基础设施。然而，令人不安的是，考虑到美国高度数字化的现状，军队和国家的基础设施和关键系统都搭建在互联网上，美国也可能成为最容易受到攻击的国家之一。一个国家如果能将削弱网络能力的攻击整合到一个综合的作战计划中，就可能在战争的初期就取得巨大的胜利。

在网络领域，不确定性比比皆是。美国防火墙通常是可以被攻破的，系统密码是可以轻易破解的，缺乏双因子认证（two-factor authentication system）的系统也带来许多复杂的漏洞。其次，网络漏洞不是静态的，它们总是在博弈中不断发展。任何网络攻击的连锁反应往往不容易预见，即使发现了具体的漏洞，仅仅通过检查个别漏洞来评估这些可能性是困难的。总的来说，美国包括私营部门的网络系统、国家民用基础设施和武装部队的系统的安全都是令人担忧的。国防科学委员会（Defense Science Board）最近的一项研究指出，几乎没有一个美国武器装备的网络系统可以被自信地视为在面对敌人的攻击时具有韧性。

造成信号中断的攻击将更具威胁性。信号干扰（jamming）、对海底光缆以及卫星的攻击、对无线电和其他通信系统软件的网络攻击，都令人非常担忧，更不用说高空核感应电磁脉冲了（high-altitude nuclear-induced electromagnetic pulse）。正是出于这种担忧，位于佐治亚州本宁堡的美国陆军优秀机动中心（Army's Maneuver Center of Excellence）正在研究未来军事行动，探索如果一个旅在很长一段时间内与师部或军团总部隔绝，并且在这段时间内必须完全依靠自己的力量运作时，应该怎么应对。

作者信息

Erol Yayboke 是美国国际战略研究中心（CSCI）弱点与流动性项目（Project on Fragility and Mobility）主任兼高级研究员。

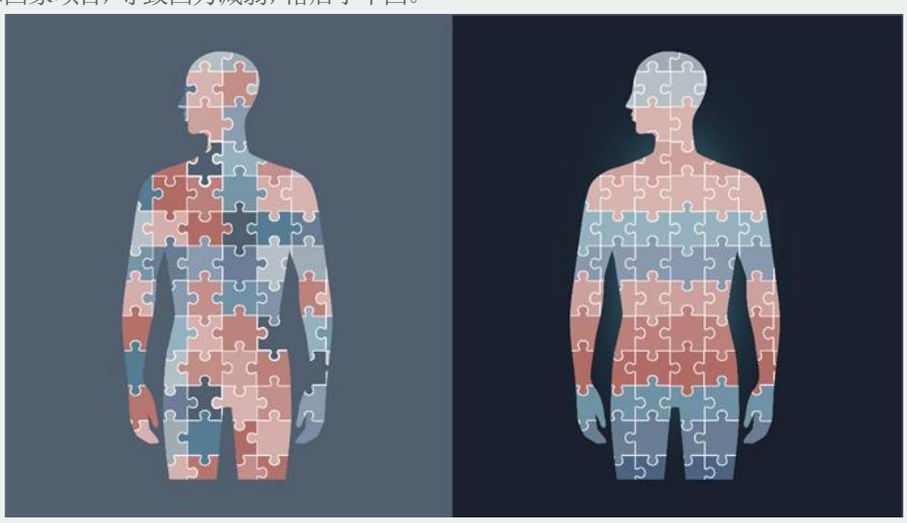
基因组：故意操纵的时代开始了

Genomes： The Era of Purposeful Manipulation Begins

■ 发布者：Carol Kuntz ■ 发布时间：2022年7月 ■ 发布机构：战略与国际研究中心
（CSIS，Center for Strategic and International Studies）

摘要 ABSTRACT

与许多新兴技术一样，基因组操纵（genome manipulation）可以发展成为一个重要的经济产业，推动创新，并有利于美国在国内外实现其战略性计划。美国需要在政策上让可遗传的人类基因组编辑合理化，明确合法的编辑类型，为制定反对非法编辑的国际规范做出贡献。美国应确保关键的硬件在国内建立和维护，如大型的、精心搭建的数据库和生物工厂。国防部需要对其对待新兴技术的措施进行结构性改革，特别是通过为军队里的医学从业人员（uniformed practitioner）创造职业发展道路。否则，美国无法将新兴技术纳入其财政预算和国家项目，导致国力减弱，落后于中国。



2022年4月，世界第一个完整的人类参考基因组公布，它可以作为DNA测序的模板，纠正了之前参考中的错误，如缺失或错位的遗传密码。（来源：美国国家标准与技术研究所National Institute of Standards and Technology，https://www.nist.gov/news-events/news/2022/03/first-complete-human-genome-poised-strengthen-genetic-analysis-nist-study）

正文ARTICLE

技术进步所带来的技术融合让DNA分子能够被刻意操纵，以创造出具有特定特征的新生命体。这种修改基因组的能力可以创造出 "有用的 "分子，从而产生新的材料，如自我修复的纺织物、由非石油原料制成的塑料、以及各种生物传感器。该技术还可以通过编辑基因组来生产蛋白质，从煤灰等废物中提炼出稀土元素。这类技术甚至还可以为新型的疾病制造量身定做的药物，配合使用精确的医疗算法来优化不同个体的治疗方案。这类编辑会带来越来越多的变革，伴随机器学习和生物信息学的发展，推进更多生物特征的遗传根源研究。

操纵基因组的能力来自三个技术进步的融合：DNA测序，CRISPR/Cas系统（原核生物的一种获得性免疫系统，用于抵抗存在于噬菌体或质粒的外源遗传元件的入侵），以及机器学习算法。DNA测序技术使特定生物体的DNA序列得以确定。CRISPR/Cas系统利用一种天然的防御机制来防止病毒的入侵，可以用来确定基因序列中需要修改的位置和具体的变化。机器学习算法凭借其在超大量数据量中识别微妙关联的能力，被用来预测获得特定的性状所需的基因编辑。

总的来说，编辑DNA的能力帮助建立一个规模达到每年数万亿美元的经济产业，可以生产新型材料、设计精准治疗的药物和定制化治疗方案、建设能够为战争带来变革的国家安全能力。然而，目前的美国未能从科学的进步中充分受益。尽管美国在科学发现和技术创新方面处于全球的领先地位，但它缺乏用来维持其领先地位，并将科学发现转化为前沿的技术应用的数据库、生物工厂以及技术劳动力。中国作为美国的一个战略竞争对手正在崛起，正伺机利用美国政策出台的延误或失误，超越美国。

美国国家制度所决定的技术发展劣势

第一，机器学习需要大型的、精心搭建的数据库。在美国，为有目的的基因组操纵（purposeful manipulation of genomes）创建数据库因许多因素而变得复杂，包括分散的医疗保健系统、公民隐私权和所有权等。另一方面，在中国，政府可以获得公民专有数据，不承认个人相对于政府的隐私权，并“通过合法和非法的手段从美国和全球各国收集大量的医疗数据集，蔑视海外知识产权”。

第二，利益因素导致关键能力外流，从而导致了发展劣势。美国私营公司追求最低成本的做法，已经使美国失去了一些关键的能力，包括开展大规模、低成本的DNA测序。例如，美国的公司几乎垄断了用于DNA测序的机器生产，但美国工业界仍然依靠中国来进行测序，以获得大规模、低成本的DNA测序。医疗机构与中国公司签订合同，让中国为他们提供DNA测序服务，中国在大规模、低成本DNA测序技术上的主导地位让中国获得美国的基因组数据。

第三，机器学习算法和相关生物技术的创新并不是由非政府主导的，而是由学术研究人员、风险资本资助者、生物技术创业公司等非政府人员或部门在国际商业集团大量资金的支持下进行的。虽然美国因其领先的学术和商用科技在各种国际专家委员会都有出席，但这些专家建议不一定会被纳入政府的政策和战略中。另一方面，中国政府始终参与科技发展的研讨，主要是因为中国公民必须与政府共享科技发展的信息。

第四，人类基因组的编辑引发了深刻而令人不安的伦理和文化问题，不同的政府和社会可能对此有不同的反应。例如，在美国，大多数可遗传的人类基因组编辑（heritable human genome editing，HHGE）研究是被禁止的，其中包括国际科学规范允许的许多研究。与此同时，尽管中国在2018年惩罚了编辑双胞胎基因组的科学家贺建奎，但它仍然允许研究可遗传的人类基因组编辑。

人工智能将比其他任何新兴技术更能改变制药业。（来源：Shutterstock.com，https://www.pharmaceutical-technology.com/analysis/new-generation-ai-drug-discovery-companies/）

四项必要的改革

第一、在美国国防部内部进行结构改革，加快采用尖端技术的能力，为新兴技术专家打造职业发展道路。美国国防部的科技生态系统太过专注于内部，不适合理解、获取和应用企业和学术部门开发的尖端技术。因此，国防部需要加强纳入外部正在迅速发展的技术的能力。最重要的改革是为专注新兴技术的军中技术人员（uniformed practitioner）建立职业发展道路。确保在少量中高级军官职级（0-5级，空军和陆军的中校或海军指挥官以上）中保留少数职位，让军中技术专家在他们的职业生涯的末期可以到达这部分级别，还可以设立一个二星级别的技术专家职位，让其直接为参谋长联席会议（Joint Chiefs of Staff）的主席提供建议。

在这个级别上，军官可以参与国防部对未来战争的性质以及未来战争的计划和预算进行讨论。国防部正在努力在其军队中培养某些类型的技术专家，但技术和军事上涉及的范围都过于狭窄，无法让国防部将新兴技术纳入其作战计划。

同时，国防部需要认真思考保密策略所带来的利弊。国防部的一些保密要求导致其在发展新兴科技上的落后，特别是在全球化商业和学术领域迅速发展的技术。DNA测序、CRISPR/Cas系统和机器学习技术就属于这种情况。国防部应该转向有快速适应能力的总体战略，跟进这些技术的最新进展，从而迅速配置应对新的战争方式的措施。

第二、建立可遗传的人类基因组编辑相关的国际规范，让美国的研究合法化，抵御他国的非法研究。国际学术专家已经阐述了一些关于可遗传人类基因组编辑的建议，世界卫生组织也试图制定一个流程来采纳这些建议。但它们的广泛采用需要在美国国务院的领导下推动。

第三、推动数据库的搭建。在生命科学研究和公共卫生领域，美国缺乏机器学习训练所需要的大型数据库。美国政府应该修改法律，建立激励机制，使重要的数据可以从数据库中获得，同时保护数据不被不当使用。特别重要的两类数据是民众的健康信息和制药公司的专有数据。应用现存的技术方法让病人的数据更广泛地用于机器学习，但同时保护病人的隐私并使病人能够决定是否授权该数据用于研究。同样地，应该建立一些数据库访问的经济激励机制，吸引企业以发展机器学习技术为目的分享药品数据。

美国政府需要创建一套新的公私合作模式。用于公共目的的数据库，特别是那些包含病人数据等敏感信息的数据库，需要由一个国家实验室或一个研究型大学联盟等非营利组织来管理，以确保对数据的适当保护和使用。同时需要私营企业的参与，只有它们才掌握了搭建大型数据库的能力。再者，应该由一个政府的高级别代表来决定各界对数据的需求是否是用于正当科研目的。

第四、利用"大挑战"竞赛，推动基因技术的发展。政府应通过组织和资助一项或几项"大挑战"（Grand Challenges）科技竞赛来加快推进转基因分子技术的发展，获得有益的经验和资产，以解决有挑战性的国家目标。

作者信息

是美国战略与国际研究中心（CSCI）战略技术项目（Strategic Technologies Program）兼职研究员。

2035年以后的新兴技术： 基于场景的未来军事突发事件技术评估

Artificial Intelligence and Arms Control

■ 发布者：Bryan Boling等 ■ 发布时间：2022年10月 ■ 发布机构：兰德公司
（RAND Corporations）

摘要 ABSTRACT

本报告介绍了一个技术评估框架，以帮助美军了解关键新兴技术的影响，这些技术可能对美军在2035年至2050年的任务至关重要。这项报告旨在帮助美军为不断变化的作战环境做好准备，例如评估面对气候变化驱动的极端天气条件下的作战方式，让新兴技术帮助美军在关键任务中取得成功并为美国带来利益。报告中以中国为假想敌，设置一个在北极地区与中国发生武装冲突的场景来模拟技术评估的开展。

美国美军未来司令部（Army Futures Command）希望有一家承包商能够为地面士兵开发更多的IT能力，包括5G、传感器、生化武器装备等前沿技术。
（来源：Washington Technology 杂志，https://washingtontechnology.com/contracts/2022/02/how-bring-more-tech-soldiers-arm-futures-command-wants-know/361845/）

正文 ARTICLE

未来是非常不确定的，对美国陆军（Army，以下简称美军）来说，预测未来全球和技术发展趋势是非常重要的。这项预测工作是为了协助美国美军为极端天气条件下的作战环境做好准备。新兴技术可能有助于美军在关键任务中取得成功并为美国带来利益。我们的具体方法侧重于基于场景的技术评估（scenario-based technology assessment），以“北极深渊之战”（Battle of the Arctic Depths）（以下简称为北极深渊）的场景为例进行分析。

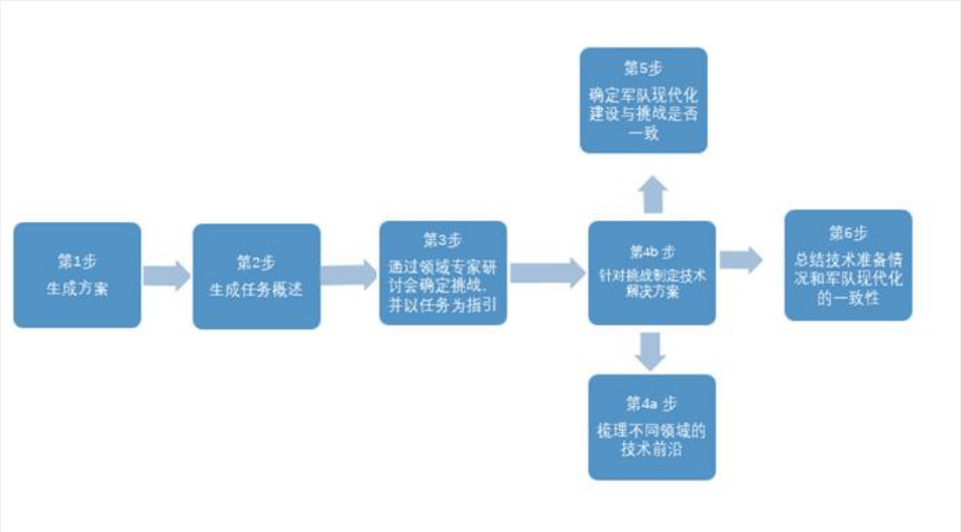
技术评估过程

首先，在步骤1中需要制定一个情景。在北极深渊的场景中，美国及北约盟友发现自己在北极地区与中国发生武装冲突。冲突是在一次科学探索旅行的幌子下开始的，中国军队在这次旅行中在丹麦的领土上插上了国旗，并声称拥有大片北极领土的主权。

步骤2是情景的一个关键组成部分——任务概述，列出完成任务所需的具体环节。北极深渊需要在严酷的环境中部署大型军事行动，以监视中国军队，将其驱逐出该地区，并长时间监视。步骤3，对于这些活动中的每一项，列出必须克服具体的挑战以完成任务。

步骤4a，我们对前沿技术分别进行了梳理，其中包含多个领域，例如，物理、生物和信息等领域。在步骤4b中，我们努力将这些技术作为步骤3中确定的挑战的潜在解决方案。在步骤5中，我们确定了当前美军现代化（Army modernization）的发展程度，以使这些成果也与挑战一一对应。

最后，在步骤6中，我们从多个方面评估技术的可用性，包括技术的总体准备情况、与其他技术的相互依赖程度、技术发展的方向、美军现代化建设的优先事项（Amry modernization priorities）是否与技术发展相一致以及技术的发展能否满足当下的需求。研究中对润滑剂、量子技术、太空运输、飞行器、自动化武器系统（autonomous weapon systems，AWS）和生物科技等领域进行了详细分析，并在以下总结：



· **润滑剂：**润滑剂可以减少摩擦、磨损和能耗，因此每台机器的运行都需要润滑剂。在寒冷的天气里，机器的粘度变得非常令人担忧。因此，近年来，在极度寒冷的条件下（如北极地区）与润滑油有关的研发工作有所增加，生产了大量具有理想性能的润滑剂和润滑脂。汽车和海运业都在这一领域进行投资，美军也投资于新的润滑剂的开发，例如单一通用动力传动系统润滑剂（Single Common Powertrain Lubricant，SCPL）是一种合成的、全季节、省油的重型发动机油，专门针对北极地区。因此，尽管单一规格的润滑油在其他工作环境中的运行效率可能较低，但SCPL会满足北极地区的挑战。

· **量子技术：**量子技术主要有三种应用——计算、通信和传感。美军正在对量子技术进行大量投资。美国美军作战能力发展部（Army Combat Capability Development，DEVCOM）和美军分布式量子信息研究实验室中心（Army Research Laboratory's Center for Distributed Quantum Information）率先开展的工作，重点是改善传感设备和建立量子通信网络。最近美军研究办公室（Army Research Office）和国家安全局物理科学实验室（National Security Agency's Laboratory for Physical Sciences）建立研究中心作为国家量子计划（National Quantum Initiative）的一部分，旨在加速和推进量子技术进入研究和军事应用。

· **生物技术：**生物技术能够增强作战装备，优化作战人员的健康和表现，并改善军事医学。美军正在大力投资于生物技术，特别是合成生物学，它是美军内部和整个国防部的优先研究领域。美军研究实验室（Army Research Lab）设立 "军事环境转化合成生物学基本研究计"（Transformational Synthetic Biology for Military Environments Essential Research Program），重点关注自组装和自我修复材料、主动伪装以及能够按需自生产的小型材料。美军的工程研究与发展中心（Engineer Research and Development Center，ERDC）曾经对微生物进行基因改造以实现生物检测和污染物（如溢油、弹药）降解。在合成生物学之外，外骨骼等外部设备的研究也有了重大进展，这些设备可以增强士兵在恶劣环境中的力量和能力。

· **地球点对点太空运输（Space Transport for Earth P2P）：**航天部门正在研发太空点对点（space P2P）技术，用于从一个点到地球上另一个点的运输。商业部门正在努力改进该技术，以提高推进（propulsion）和着陆（landing）过程，降低飞行器发射、回收和翻新的成本，并满足商用的安全标准。该领域很大程度上取决于商用技术的发展。美国空军（U.S. Space Force）正在开展火箭货物先锋计划（Rocket Cargo Vanguard program），以利用市场对太空点对点技术的开发。

· **飞行器（air vehicle）：**飞行器的垂直起飞和降技术（vertical take-off and landing，VTOL）并不是一项新技术。传统的直升机和旋翼机，如 "支奴干"（Chinook）和 "黑鹰"（Black Hawks），数十年来一直作为VTOL空中交通工具为军队服务。如旋翼、推进器、带有人工智能和先进传感器的态势感知、航空电子设备、通信和先进复合材料等关键技术领域正在取得进展。尽管VTOL技术对于类似于北极情景下的任务来说肯定是有吸引力的，但目前对于与北极情景下所需要的重型和超重型有效载荷飞行器的开发还很欠缺。

· **自动化武器设备（autonomous weapon systems，AWS）：**尽管国际上对自动化武器的应用缺乏共识，但美军正在积极发展该领域，例如投资半自主和自主车辆和武器系统的研究。

北极深渊场景下的技术评估发现

许多美军现代化技术的优先发展事项能够应对美军在设想中所面临的关键挑战，包括自动化武器，生物科技和量子技术。这有助于为技术成熟后与作战行动整合打下基础。

然而，目前美军的一些优先发展的现代技术与北极深渊情景中的挑战不适配。1) 就润滑剂而言，美军正在追求单一规格的润滑剂，而商业部门的发展正在为特定的操作环境推进润滑剂技术。2) 在北极深渊的场景中，垂直起飞和降落飞行器需要重型起重能力，而美军目前专注于轻型和中型起重航空资产的垂直起飞和降落技术的发展，与预期存在差距。

美军的优先发展事项与点对点太空运输技术方面的潜在需求不一致。未来可以由商业部门推动美军在这一领域的发展。

因此，建议美军未来司令部 (Army Futures Command，AFC) 可以考虑通过美军总部和美军物资司令部（Army Materiel Command），在能源、太空运输等私营产业中的领头企业和国际伙伴建立合作关系，以确保通过技术评估确定为关键的技术的可用。

关于技术评估的建议

进行技术评估的目的是提供一个关于技术如何应用于未来场景的前瞻性分析，因此需要通过制定具体场景，提供一个可以对技术进行评估的特定未来。

为这些场景进行技术评估，必须考虑具有高度不确定性的技术，应用领域内的专家评估技术成熟程度、影响和可用性。

技术评估应该有一个系统化的过程，提供一个可重复的分析流程，将场景切分为不同的任务和挑战，应用技术解决挑战，并根据候选技术解决方案评估军队现代化技术的发展状况。

作者信息

Bryan Boling是兰德公司（RAND Corporations）工程与应用科学部的工程师，也是航空航天工程博士。

太空的军事化

The Militarization of Space

■ 发布者：Claire Mills ■ 发布时间：2021年6月 ■ 发布机构：英国下议院图书馆
（House of Commons Library, UK Parliament）

摘要 ABSTRACT

过去几年中，世界各国在太空中不断进行各种各样的研发活动，军事、民用和商业航空部门之间日益相互依存。国际上对太空行为缺乏监管和公认的国际准则，推进这一议程的国际意愿也不强烈，加剧了人们对未来军备竞赛的担忧。本简报探讨了太空军事化如何演变为太空武器化，以及各国各自扮演什么样的角色。

美国国家航空航天局（NASA）在地球上空的国际空间站。
（来源：英国肯特大学，https://www.kent.ac.uk/news/society/18567/donald-trumps-space-force-the-dangerous-militarisation-of-outer-space）

正文 ARTICLE

几十年来，太空一直被用于军事目的，但仅限于部署通信、导航、成像和监视卫星等非进攻性军事系统。包括英国在内的几个国家通过其卫星通信系统开发了一套综合的太空军事架构，以推动地面军事活动。过去几年中，世界各国在太空中不断进行各种各样的研发活动，军事、民用和商业航空部门之间日益相互依存。包括俄罗斯和中国在内的少数国家，在攻击性反太空能力（counterspace capabilities）方面进行了大量投资，这可能威胁到英国及其盟国在太空中的活动。因此，保护重要的民用和军用太空资产已成为一项优先事项，太空军事化也正在逐渐演变为太空武器化。

太空中的军事资产在哪里？注：本节介绍的数据更新至2022年5月1日。

根据美国关切的科学家联盟（Union of Concerned Scientists）公布的最新数据，在太空中有5,464颗人造卫星，遍布整个太空光谱。估计86%（4700颗）人造卫星在低地球轨道（low earth orbit，LEO）。10.3%（565颗）在地球同步轨道（geosynchronous earth orbit，GEO），也被称为地球静止轨道（geostationary orbit）。2.6%（140颗）在中地球轨道（medium earth orbit，MEO）。

在这些人造卫星中，10.6% (577颗) 用于军事目的。其中一半以上 (319颗) 是在低地球轨道。低高度和短轨道周期的特点使低地球轨道军事卫星成为地球观测、成像、监视和侦察的理想选择。

大约四分之一的军用卫星 (137颗) 在地球同步轨道上。在这个轨道上的卫星和地球的旋转周期是同步的，这使它们成为天气监测、情报观察和构建通信系统的理想选择。许多机密的军事卫星都在地球同步轨道上。

还有94颗军用卫星在中地球轨道上。中地球轨道上的卫星比低地球轨道上的卫星有更大的地理覆盖范围，而比地球同步轨道上的卫星信号传输时间更短，普遍用于导航系统。美国的导航卫星全球定位系统 (Navstar GPS)、俄罗斯的格洛纳斯系统 (GLONASS)、中国的北斗系统和欧盟的伽利略系统 (Galileo) 都在这个轨道上运行。

资料来源：美国陆军采办支持中心（US Army Acquisition Support Center）

轨道类型	高度（千米）
低地球轨道（LEO）	高达约 2000
中地球轨道（MEO）	约 2000-35000
地球同步轨道(GEO)	约 35000

什么是反太空能力?

人们普遍认为，反太空能力或太空对抗能力 (counterspace capabilities) 是那些可以用来破坏、排斥、降级或摧毁太空系统的能力。这些能力在性质上可以是动能的 (kinetic，涉及对太空资产进行直接的物理攻击或对一个物体进行物理干扰，使其脱离稳定的轨道) 或非动能性的 (non-kinetic，对一个目标产生影响而没有实际的物理接触)。反太空行动利用数据和软件瞄准想要攻击的太空系统，通过干扰 (jamming) 或电子欺骗 (spoofing) 或网络入侵等手段，破坏太空设备的传输和接收能力。这些能力可以是地面发射的 (地球到太空)，基于太空的 (太空到太空) 或攻击地球上的目标 (太空到地球)，包括:

· 直接升空的反卫星 (ascent anti-satellite，ASAT) 导弹 (地球到太空)。它们能够瞄准低地球轨道上的卫星，如果射程足够大，也可能瞄准中地球轨道上的卫星。
· 共轨反卫星武器 (太空到太空)。
· 地面或太空定向能武器 (directed energy weapon)，如激光、微波、电磁脉冲。
· 针对卫星和相关地面基础设施的网络攻击或电子战 (electronic warfare)，如上行卫星干扰。
· 太空导弹拦截器和全球攻击能力，旨在针对地球上的特定地点。

太空的管理

在发展太空武器方面，1979年《月球协定》(Moon Agreement) 第三条禁止在月球上制造威胁或使用武力，同时禁止在绕月轨道上放置核武器。然而，《月球协议》只有18个缔约方，其中不包括英国、美国、俄罗斯和中国。当涉及到将武器或军事设备放入地球周围的轨道，现存规定对军事化的限制是有限的。《外层空间条约》(Outer Space Treaty) 第四条规定，目前只有核武器或大规模杀伤性武器不得进入围绕地球的轨道，但它并不禁止将其他武器和军事装备放入地球周围的轨道。

在太空中拥有卫星的国家 (单位: 个)
2022年5月1日太空卫星所有者或经营者中排名前十的国家

国家	#商业	#民用	#政府/军事	共计
美国	3109	64	426	3449
中国	172	32	344	541
英国	482	1	10	490
俄罗斯	74	9	127	173
日本	39	20	39	97
欧洲航天局	30	1	35	65
印度	2	4	59	63
加拿大	43	5	15	59
德国	12	20	21	48
卢森堡	41	0	1	42

注：一颗卫星可以有双重用途，例如既用于商业也用于军事。
资料来源：关切的科学家联盟，UCS卫星数据库（Union of Concerned Scientists, UCS Satellite Database）。

当下的国际法缺乏太空军事化相关的规定，然而就监管达成共识并不容易。世界上主要的太空大国对监管应该是什么样子以及它应该实现什么目标都有自己的解释。美国一贯投票反对任何旨在通过更正式的条约机制防止太空军备竞赛的联合国决议。俄罗斯和中国都因长期以来支持对太空军备控制的而受到批评，它们同时也在建立反太空能力，包括反卫星能力等被广泛认为是带有挑衅和破坏稳定的行为。

美国

在过去20年，美国一直对太空的所有要素进行研究和开发。关于进攻性反太空能力的研究集中在动能和非动能的反卫星 (ASAT) 能力、定向能武器和电子战。作为修订后的导弹防御计划的一部分，太空拦截器的潜在作用也被重新评估过几次。在21世纪初，美国还对在太空部署常规快速全球攻击 (conventional prompt global strike) 能力进行了研究。

美国在太空中拥有世界上最广泛的态势感知 (situational awareness) 能力。其核心是一个地理上分散的地面远程雷达 (ground-based long-range radars) 和望远镜网络，太空望远镜，以及地球静止轨道上的红外卫星 (infrared satellite) 网络。红外卫星中最新的一代是天基红外系统 (Space-Based Infrared System，SBIRS) 。

美国没有专门的直接升空反卫星 (direct-ascent ASAT) 能力。然而，它拥有可运行的中段导弹防御拦截器 (midcourse missile defense interceptor)，过去曾证明这些拦截器对低地球轨道上卫星能够发挥反卫星作用。因此，如果需要，这些拦截器可以提供这种能力。虽然美国目前没有一个公认的发展共轨 (co-orbital) (太空到太空) 能力的计划，但作为其反卫星试验和早期导弹防御计划的一部分而被开发的技术能力，足以使美国在相对较短的时间内发展共轨反卫星能力。

美国有一个在全球部署的电子战反太空系统 (Counter Communications System, 反通信系统) , 并有可能对地球静止通信卫星提供上行链路干扰能力。美国军方也有能力干扰全球导航卫星服务的民用信号, 如俄罗斯格洛纳斯系统 (GLONASS) 和中国北斗系统。

2020年6月, 美国国防部发布了最新的《国防太空战略》(Defence Space Strategy) , 提出了四个主要目标: 1) 在太空建立全面的军事优势; 2) 将太空军事力量纳入国家和国际联合行动; 3) 塑造太空的战略环境; 4) 与盟友、伙伴、各产业和其他美国政府部门机构在该领域合作。

2021年5月28日, 拜登政府提出了国防部2022财政年度的预算请求。该请求指出206亿美元将被分配用于加强美国在太空的能力。2000万美元还被分配用于建立国家太空情报中心 (National Space Intelligence Center) , 并对外太空 (deep space) 先进雷达增加了投入资金, 以探测和跟踪外太空物体。美国空军预算副助理部长 (US Air Force Deputy Assistant Secretary for Budget) 詹姆斯-佩奇亚 (James Peccia) 少将指出, 今年有远远超过8亿美元的机密项目进入太空部队。美国导弹防御局 (US Missile Defense Agency) 22财年的资金申请还包括2.92亿美元用于提高太空态势感知能力。

美国太空部队正准备将太空军事化。
（来源：美国华盛顿邮报，https://eppc.org/publication/the-u-s-space-force-is-preparing-to-militarize-space-good/）

俄罗斯

在过去的几年里, 俄罗斯因一系列反卫星试验而被登上新闻头条, 这表明俄罗斯在发展直接上升反卫星 (direct-ascent ASAT) 导弹计划和共轨反卫星 (co-orbital ASAT) 能力方面取得了重大进展。2020年7月, 美国及其盟国指责俄罗斯对一枚天基反卫星武器进行了进一步的无损检测, 当时一颗俄罗斯卫星将一个新物体高速发射到轨道上, 该导弹可能通过动能冲击摧毁目标, 因此被视为具有武器的特性。

俄罗斯还高度重视将网络、电子战和定向能武器纳入其反太空活动。在苏联时期的遗留计划和最近投入使用的激光系统的基础上, 俄罗斯正在开发一些地面和空中激光系统, 供俄罗斯太空部队用于瞄准图像和侦察卫星。自2014年以来, 俄罗斯被指控广泛开展电子太空对抗战, 在最近的军事行动中以及在其境内, 干扰附近领土的导航和通信卫星。

中国

与美国和俄罗斯相比, 中国在太空的军事活动相对较晚。在其2016年的《太空白皮书》中, 中国提出了成为"太空大国"的长期战略目标。在过去几年里, 中国进行了最多的太空发射, 现在轨道上运行的人造卫星数量仅次于美国。中国在太空的军事努力体现在两个方面: 1) 发展自己的太空军事架构以便在地面开展军事活动和2) 发展广泛的太空对抗能力。

2007年, 中国成功发射了第一枚直接升空的反卫星导弹SC-19, 能够瞄准低地球轨道卫星。据报道, 中国在过去十年里对该导弹系统进行了升级和现代化改造, 2018年, 中国解放军组建了军事部队, 并开始进行初步的太空作战训练。据评估, SC-19现在已经投入使用。中国还被认为开发了共轨反卫星能力, 并已投入使用, 其中包括带有机械臂技术的卫星。

与俄罗斯一样, 中国也一直在大力投资非动能反太空技术, 如定向能武器和电子战。据报道, 中国已经开发了能够致盲商业和军事成像卫星的高能激光器。中国还拥有先进的网络能力, 在过去几年中被恶意指控对美国卫星进行了几次网络攻击。

英国

英国《2021年综合审查及相关国防指挥文件》提出了英国的雄心壮志，即到2030年成为 有影响力的太空参与者 (a meaningful player in space) 。在未来十年，英国国防部 (Ministry of Defense，MOD) 将投资约50亿英镑，2025年交付"天网6号"计划 (Skynet 6 programme) ，对其卫星通信能力进行资本重组和增强，并进一步投资 14亿英镑用于打造与太空相关能力。具体而言，国防部将在低地球轨道上建立一个新的情报、监视和侦察 (intelligence，surveillance and reconnaissance， ISR) 卫星群，应用光电 (electro-optical) 、红外线、合成孔径雷达 (synthetic aperture radar) 和高光谱解决方案。

作者信息

Claire Mills是英国下议院图书馆研究员。

以知识创新推动社会进步